CLAIMS

1. A method for communication path analysis, the method comprising:

retrieving a first communication path rule and a second communication path rule for an access control device, each rule comprising at least one path attribute type specifying at least one attribute and at least one path operation type specifying at least one operation;

inserting the first rule into a database;

determining, for at least one path attribute type, whether an attribute of the second rule corresponds to an attribute of the first rule; and

when the attribute of the second rule does not correspond to an attribute of the first rule, inserting the attribute of the second rule into the database, along with the at least one operation of the second rule.

2. The method of claim 1, wherein retrieving a communication path rule comprises parsing the rule from a firewall configuration file.

3. The method of claim 1, wherein the at least one path attribute type comprises one or more of destination address, source address, service type, and communication time.

4. The method of claim 1, wherein inserting the first rule into a database comprises placing the at least one attribute and the at least one operation into a relational database having separate tables for the path attribute type and the path operation type.

5. The method of claim 1, further comprising:

determining whether a database query has been received; and

if a query has been received, searching the database to determine whether any communication path rules satisfy the query.

6. The method of claim 5, wherein the query criteria comprise one or more of destination address, source address, service type, and communication time.

7. The method of claim 1, wherein:

determining whether an attribute of the second rule corresponds to an attribute of the first rule for at least one path attribute type comprises performing a set difference operation between attributes of the second rule and attributes of the first rule for the at least one path attribute type; and

inserting the attribute of the second rule that does not correspond to an attribute of the first rule into the database comprises inserting the results of the set difference operation into the database.

8. The method of claim 1, wherein inserting the attribute of second rule that does not correspond to an attribute of the first rule into the database comprises attempting to group at least one type of non-corresponding attributes of the second rule into ranges.

9. The method of claim 1, further comprising:

retrieving a first communication path rule for a second access control device; and

inserting the first communication path rule for the second access control device into the database.

10. The method of claim 9, further comprising:

determining whether a database query has been received; and

if a query has been received, searching the database to determine whether any communication path rules satisfy the query.

11. The method of claim 1, wherein determining whether an attribute of the second rule corresponds to an attribute of the first rule for at least one path attribute type is performed only for a set of operations.

12. A system for communication path analysis, comprising:

a communication rule analyzer comprising:

a database operable to store and search communication path rules, each rule comprising at least one path attribute type specifying at least one attribute and at least one path operation type specifying at least one operation; and

an extraction tool operable to:

retrieve a first communication path rule and a second communication path rule for an access control device,

insert the first rule into the database,

determine, for at least one path attribute type, whether an attribute of the second rule corresponds to an attribute of the first rule, and

when the attribute of the second rule does not correspond to an attribute of the first rule, insert the attribute of the second rule into the database, along with the at least one operation of the second rule.

13. The system of claim 12, wherein the database comprises a relational database having separate tables for the path attribute type and the path operation type.

14. The system of claim 12, wherein the database is further operable to:

determine whether a database query has been received; and

if a query has been received, search the database to determine whether any communication path rules satisfy the query.

15. The system of claim 12, wherein the extraction tool is operable to:

perform a set difference operation between attributes of the second rule and attributes of the first rule for the at least one path attribute type to determine whether an attribute of the second rule corresponds to an attribute of the first rule for at least one path attribute type; and

insert the results of the set difference operation into the database to insert the attribute of the second rule that does not correspond to an attribute of the first rule into the database.

16. The system of claim 12, wherein the extraction tool is operable to attempt to group at least one type of non-corresponding attributes of the second rule into ranges to insert the attribute of the second rule that does not correspond to an attribute of the first rule into the database.

17. The system of claim 12, wherein the extraction tool is further operable to:
retrieve a first communication path rule for a second access control device; and
insert the first communication path rule for the second access control device into the database.

18. The system of claim 17, wherein the database is further operable to:
determine whether a database query has been received; and
if a query has been received, search the database to determine whether any communication path rules satisfy the query.

19. The system of claim 12, wherein the extraction tool is operable to determine whether an attribute of the second rule corresponds to an attribute of the first rule for at least one path attribute type only for a set of operations.

20. An article comprising a machine-readable medium storing instructions operable to cause one or more machines to perform operations comprising:

retrieving a first communication path rule and a second communication path rule for an access control device, each rule comprising at least one path attribute type specifying at least one attribute and at least one path operation type specifying at least one operation;

inserting the first rule into a database;

determining, for at least one path attribute type, whether an attribute of the second rule corresponds to an attribute of the first rule; and

when the attribute of the second rule does not correspond to an attribute of the first rule, insert the attribute of the second rule into the database, along with the at least one operation of the second rule.

21. The article of claim 20, wherein inserting the first rule into a database comprises placing the at least one attribute and the at least one operation into a relational database having separate tables for the path attribute type and the path operation type.

22. The article of claim 20, wherein the instructions are further operable to cause one or more machines to perform operations comprising:

determining whether a database query has been received; and

if a query has been received, searching the database to determine whether any communication path rules satisfy the query.

23. The article of claim 22, wherein the query criteria comprise destination address, source address, service type, and communication time.

24. The article of claim 20, wherein:

determining whether an attribute of the second rule corresponds to an attribute of the first rule for at least one path attribute type comprises performing a set difference operation between attributes of the second rule and attributes of the first rule for the at least one path attribute type; and

inserting the attribute of the second rule that does not correspond to an attribute of the first rule into the database comprises inserting the results of the difference operation into the database.

25. The article of claim 20, wherein inserting the attribute of the second rule that does not correspond to an attribute of the first rule into the database comprises attempting to group at least one type of non-corresponding attributes of the second rule into ranges.

26. The article of claim 20, wherein the instructions are further operable to cause one or more machines to perform operations comprising:

retrieving a first communication path rule for a second access control device; and

inserting the first communication path rule for the second access control device into the database.

27. The article of claim 26, wherein the instructions are further operable to cause one or more machines to perform operations comprising:

determining whether a database query has been received; and

if a query has been received, searching the database to determine whether any communication path rules satisfy the query.

28. The article of claim 20, wherein determining whether an attribute of the second rule corresponds to an attribute of the first rule for at least one path attribute type is performed only for a set of operations.

29. A method for communication path analysis, the method comprising:

receiving a database query for a database comprising communication path rules for an access control device, each rule comprising at least one path attribute type specifying at least one attribute and at least one path operation type specifying at least one operation;

searching the database for rules that satisfy the query; and

generating a user interface to present the results of the search.

30. The method of claim 29, wherein the database comprises a relational database having separate tables for the path attribute type and the path operation type.

31. The method of claim 29, wherein the format of the query is structured query language.

32. The method of claim 29, further comprising populating the database.

33. The method of claim 29, wherein the database comprises a communication path rule for a second access control device.

34. An article comprising a machine-readable medium storing instructions operable to cause one or more machines to perform operations comprising:

receiving a database query for a database comprising communication path rules for an access control device, each rule comprising at least one path attribute type specifying at least one attribute and at least one path operation type specifying at least one operation;

searching the database for rules that satisfy the query; and

generating a user interface to present the results of the search.

35. The article of claim 34, wherein the database comprises a relational database having separate tables for the path attribute type and the path operation type.

36. The article of claim 34, wherein the instructions are further operable to cause one or more machines to perform operations comprising populating the database.

37. The article of claim 34, wherein the database comprises a communication path rule for a second access control device.

38. A system for communication path analysis, the system comprising:

a communication rule analyzer comprising:

a relational database operable to store, receive queries for, and search communication path rules, each rule comprising at least two path attribute types specifying at least one attribute and at least one path operation type specifying at least one operation, the database comprising separate tables for the path attribute types and the path operation type; and

an extraction tool operable to:

retrieve a first communication path rule and a second communication path rule for an access control device,

insert the first rule into the database,

perform a set difference operation between path attribute types of the second rule and the first rule,

insert the result of the difference operation into the database, along with the at least one operation of the second rule,

retrieve a first communication path rule for a second access control device, and

insert the rule into the database.